# Service Definition

## Microsoft Azure Cloud Security Strategy, Design and Risk Management Support

**Supplier:** Shivom Consultancy Limited
**Framework:** G-Cloud 15
**Lot:** Lot 3 – Cloud Support Services

shivom

## Service overview

This service provides cloud support for Microsoft Azure security strategy, secure design and security risk management. It supports public sector organisations to define security approaches, design secure Azure architectures and manage cloud security risks.

## Scope of the service

The service covers Azure security strategy development, secure architecture design, security risk identification and management. It includes advisory support aligned to Azure services and UK public sector security expectations.

## Features

Azure security strategy development
Secure Azure architecture design reviews
Azure security posture assessments
Threat modelling for Azure workloads
Security risk identification and analysis
Azure identity and access design
Network security and segmentation design
Data protection and encryption guidance
Logging, monitoring and alerting design
Security governance and control alignment

## Benefits

Clear Azure security strategy alignment
Reduced cloud security risks
Improved protection of sensitive data
Stronger identity and access controls
Better visibility of security threats
Consistent security governance approach
Improved compliance readiness
Secure-by-design Azure architectures
Reduced likelihood of security incidents
Increased confidence in Azure adoption

## Service constraints

The service is delivered remotely during UK business hours unless otherwise agreed. It provides advisory, design and risk management support only. Implementation activities, Azure licences, subscriptions and third-party tools are excluded.

## Onboarding and implementation

Onboarding includes agreement of scope, objectives and stakeholders. Implementation focuses on assessment, design and advisory activities delivered collaboratively with buyer teams.

## Service management and support

Shivom Consultancy Limited provides flexible support levels tailored to buyer needs and the criticality of the service. Level 1 support provides first-line support for service queries, incident logging, basic troubleshooting and request handling during UK business hours. Level 2 support provides second-line technical support, including deeper investigation, issue resolution and configuration support, with extended hours available by agreement. Level 3 support provides specialist and expert-level support, including complex fault resolution, architectural input and escalation handling. Support costs vary depending on the selected support level, hours of coverage and service scope. Pricing is agreed with the buyer at the start of the engagement and detailed in the call-off contract. A named technical account manager or cloud support engineer can be provided for Level 2 and Level 3 support, acting as the primary point of contact and supporting service governance and escalation.

## Offboarding and exit management

On exit, all service outputs are handed over to the buyer. Knowledge transfer sessions can be provided if required. No buyer data is retained after contract completion.

## Security and data protection

The service follows UK public sector security requirements. Access is limited to authorised personnel with BPSS screening. Buyer data is handled in line with agreed security policies.

## Accessibility

Accessibility standards align to WCAG 2.2 AA. Documentation and support materials are designed to meet accessibility requirements where applicable.

## Pricing

Pricing is agreed at call-off and depends on scope, duration and depth of financial and sustainability analysis required. All pricing is transparent and documented in the call-off contract.